ORIGINAL

JUNJI SUZUKI (SBN 184738)
junji@marshallsuzuki.com
MARSHALL SUZUKI LAW GROUP, LLP
230 California Street, Suite 415
San Francisco, CA 94111
Telephone: (415) 618-0090
Facsimile: (415) 618-0190
Attorney for Applicant,
Medical Corporation H&S

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

VKD

In re Ex Parte Application of

Medical Corporation H&S,

Applicants.

Case No: CV-19-80186MISC

DECLARATION OF TAKU INOUE IN SUPPORT OF EX PARTE APPLICATION FOR ORDER PURSUANT TO 28 U.S.C. § 1782 PERMITTING DISCOVERY FOR USE IN FOREIGN PROCEEDING

BY FAX

I, Taku Inoue, declare as follows:

1. I am an attorney duly licensed to practice law in Japan.
2. I have personal knowledge of each matter stated herein.
3. I submit this declaration in support of Medical Corporation H&S (the "Applicant")'s ex parte application for order pursuant to 28 U.S.C. § 1782 (the "Application").
4. I have reviewed the Application and other supporting documents concurrently submitted herewith and am familiar with the matters stated in those documents. The purpose of this declaration is to explain the need for disclosure of all access logs held by a Content Provider (defined below) in order for the Applicant to identify an anonymous perpetrator who posted illegal statements (e.g. defamation and unlawful business interference) on the internet, in case the Court may wonder if the duration for access logs should be limited.

5. Explanation of Terms

An Internet Service Provider (the "ISP") is an entity such as AT&T which provides internet services for users. A Content Provider (the "CP") is an entity which provides content on the internet. If a user accesses a Google map review page by using AT&T line, the ISP is AT&T and the CP is Google LLC ("Google").

In the case of above example, at first, the communication between the user and AT&T is performed before the communication between AT&T and Google is performed. In each communication, information such as IP addresses, time stamps (the time when they were used for the communication) and access types are generally recorded. This record is called an "access log". See Exhibit A and B.

The ISP assigns (lends) an IP address to its user when providing the user with internet access services. The IP address assigned (loaned) to the user is changed at set intervals. Thus, the ISP can identify the user by IP address and time stamp (in other words, the access log).

6. How to Identify the Perpetrator by Using the Access Log

The victim can identify the perpetrator by using the access log as follows:

(1) The victim of illegal activity on the internet does not know the ISP the perpetrator used. Thus, the victim needs the CP to disclose the access log in their possession. The Applicant submits the Application for that purpose. See Exhibit A (1).

(2) Next, the victim identifies the ISP the perpetrator used by the IP addresses disclosed by the CP. Since IP addresses owned by a particular ISP are publicly available, such IP addresses help the victim identify the ISP used by the perpetrator. See Exhibit A (2).

(3) Next, the victim submits the access logs (including IP addresses and time stamps) disclosed from the CP to the ISP, and requests the perpetrator's information such as his/her name and address. See Exhibit A (3).

(4) In this way, the victim is able to obtain the perpetrator's information from the ISP. See Exhibit A (4).

(5) Finally, the victim is able to sue the perpetrator. See Exhibit A (5).

Strictly speaking, there is a gap between time stamps recorded by the ISP and those recorded by the CP because of the time needed for communication between the ISP and the CP. However, this gap is negligibly small and should therefore not present any issue.

7. The Necessity of Disclosure of the Access Log by the CP

In almost all cases, the CP does not have accurate information necessary to identify the perpetrator. First of all, the CP does not obtain the perpetrator's name or address unless the perpetrator volunteers them for using services by the CP. In addition, there is a high possibility the information the CP may receive from the perpetrator at the time of his/her registration for use of the CP's services is fictitious, especially in case of illegal purposes such as posting illegal statements. Thus, in almost all cases, the victim has to rely on the method described in paragraph 6 above to identify the perpetrator. In other words, in almost all cases, having the CP disclose an access log is the only way to identify the perpetrator. That is why the access log from the CP is critically necessary.

8. All Access Logs Without Duration Limit Need Be Disclosed

Ideally, a single, complete access log should be readily available to enable the victim of defamation on the internet to identify the perpetrator. However, the access log at the time of posting is not always complete, nor does it remain available indefinitely, as explained below. (See Exhibit B). At the same time, it is impossible for the CP to identify a single access log from which all the information needed by the victim can be extracted because of the existence of special tools for anonymization (explained below).

As to completeness of a particular log, it is unclear how the provider maintains access logs. For example, some providers such as Google often records only time stamps (not IP addresses) at the time of each posting. In that case, the victim is unable to identify the ISP, which means that the victim is unable to identify the perpetrator, either.

As to how long a particular log remains available, the "freshness" of the log is important. If the perpetrator posted an illegal statement (e.g. defamatory comment) several months ago, the CP or the ISP may have already deleted the access log at the time of posting. Generally, the retention period of access logs by providers is only 3 to 6 months. Thus, in a large number of cases, the access log at the time of posting has already been deleted by the time a subpoena can be served on the CP or the ISP. In addition, even if the access log at the time of posting remains available and disclosed by the CP, there is a possibility that the ISP has already deleted the access log when the victim asks the ISP to disclose it.

It should be noted that the perpetrator can prevent the victim from identifying him/her through access logs by using special tools for anonymization such as Tor (The Onion Router) or Proxy (collectively, the "Special Tools"), mainly used in the dark web. The perpetrator sometimes uses the Special Tools and at other times does not. The victim can possibly identify the perpetrator from the access logs only if the perpetrator does not use the Special Tools. The victim (and the CP), however, cannot specify access logs from which the information sought may be ascertained because the victim does not know when and whether the perpetrator used the Special Tools.

Therefore, all access logs, including the most recent logs, need be disclosed as long as they are presumed to be those of the same perpetrator. For example, access logs identifying the same Google account of the perpetrator are presumed to belong to the perpetrator.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Dated: July 16, 2019

By: Taku Inoue
Taku Inoue

Exhibit A

How to Identify the Perpetrator by Using Access Log

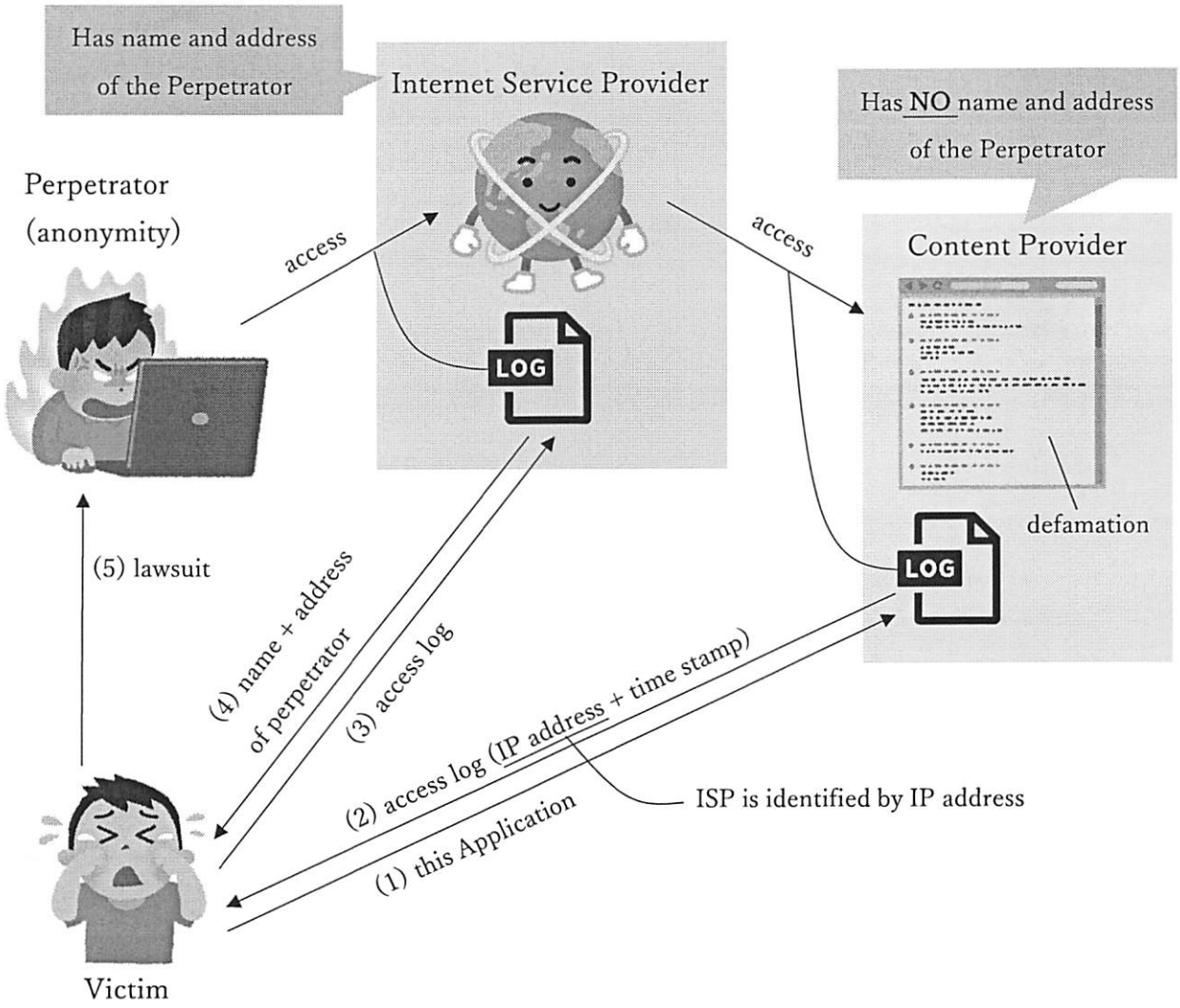

Exhibit B

Sample of Access Log

Access Log as of 2018/12/31

Time Stamp	IP address
2018/12/29-23:50:45-UTC	Unknown
2018/11/28-21:40:35-UTC	123.456.789.12
2018/10/27-19:30:25-UTC	Unknown
2018/09/26-17:20:15-UTC	123.456.789.12
2018/08/25-15:10:05-UTC	987.654.321.98
2018/07/24-13:00:55-UTC	Unknown
2018/06/23-11:50:45-UTC	987.654.321.98
2018/05/22-09:40:35-UTC	987.654.321.98
2018/04/21-07:30:25-UTC	Unknown

Server does not always register full information of access log

Victim does not know which access log is sufficient to identify the perpetrator

Access log at the time of posting

There is a possibility that server has already deleted these access logs

There is a high possibility that server has already deleted these access logs